No. 6,205,436 to Rosen. This rejection is respectfully traversed because neither Fleming nor Rosen disclose or suggest an electronic withdrawal authorization store and forward system or method for cash and credit accounts.

Applicant's independent claims 1 and 10 recite a system and method, respectively, for collecting, storing and forwarding account approval information which enables account withdrawals and charges by someone other than an account holder. According to claim 1, the system comprises:

> "a) an input terminal in which a source accountholder provides data indicating a source account at an institution from which funds will be paid, a cap value on the amount of the funds to be made available, authorization, and a secret code, all of which is transmitted to:
>
> b) a trigger server which stores account information, authorization and secret code; and
>
> c) a requesting terminal at which the first person to enter the secret code is provided the source account approval information for a transaction up to the cap limit to the institution in which the previously provided source account is maintained."

While seemingly simple and straightforward, this system is neither disclosed nor suggested by Fleming or Rosen, or by any other source known to the applicant.

The Fleming patent describes a set of "parent and child" accounts where the owner of the parent account is liable for, and holds control over the expenditures for the child(s) account(s). Also, the holder of the master account is the one responsible for paying for charges generated by the child(s) account(s). It is a system that works much like a corporate credit card where the main accountholder (the corporation) pays for the charges of it's employees' corporate cards with some extended control over the limits on the usage of each child's credit card account.

The Fleming system lacks scalability when dealing with allowances to individuals not previously specified by the account holder. As an example, in order for an accountholder to authorize someone to execute a $20 transaction, a separate child's account for that individual has to have been previously created and linked to the accountholder's parent account. Also, the whole concept of anonymity for the person effectuating the purchase disappears once the individual performing the transaction is required to be another registered accountholder of a child account, linked to the parent account.

Over distributed environments like the Internet, such a parent/child account solution proves to be impractical due to its lack of scalability and registration requirements, forcing the creation of one child account per each target user prior to using the system. Such registration process also completely destroys any possibility of anonymity by the individual performing the subsequent sales transaction, distancing it even further from the "trigger system" of the applicant.

The Rosen patent discloses a system for purchasing goods or services between two trusted agents and money modules wherein, once agreed upon, the transaction cannot interfere with either the delivery of the goods or services, or with the delivery of the payment between the trusted agents and the money modules. It discloses a contractual system wherein, once the transaction is electronically committed, neither the merchant nor the customer can interfere with the outcome of the transaction.

With Rosen's system both agents bear liability for the conditions established on the electronic contract, one for the delivery of the goods or services and the other for delivery of the payment.

The "trigger system", according to the invention, differs from Rosen's system in that, on a trigger transaction, neither goods or services nor payments are involved. The trigger system is solely concerned with authorizations (credentials) without knowledge of the context in which such credentials will be subsequently used.

With the trigger system, no monetary transaction is effected and nothing, aside from storage and delivery of someone's account authorization, is accomplished. Its whole purpose is as a support system for other regular sales transactions (as in Rosen's or Fleming's systems) avoiding liabilities and implications related to the delivery of goods and payments simply by not participating in such transactions where a sale is made against payment.

Both Fleming and Rosen describe electronic sales transaction systems for delivery of goods and/or acceptance of payments between customers and merchants based upon electronic agreements. In contrast, the trigger system implements a method for storing and forwarding financial credentials only, which can be delivered to other systems in triggered transactions that do not constitute either a sale or a payment.

Of course, trigger transactions occur with the intention of being used in subsequent "sales transactions" for the purchase of goods or services; however, the trigger transaction itself does not effectuate any sale and therefore does not generate any liability to the server or device supporting it. Its only responsibility is to make sure that the financial credentials will be stored safely and will be delivered only upon completion of certain requirements.

In the Examiner's view, as stated in numbered paragraph 4, page 3 of the Office Action:

> "The motivation to combine [Fleming and Rosen] is to teach a system to permit remote delivery of electronic merchandise or service with real time anonymous payment or real time authorization based payment where neither the customer nor the merchant can interfere with the payment and delivery process once they have agreed to the transaction as enunciated by Rosen."

Applicant respectfully submits that it is not at all obvious to combine two systems meant to transact goods, services and payments -- where liabilities and settlements are mandatory by both parties involved and no anonymity is possible -- to come up with a separate system where no sales transactions occur, full anonymity is achievable and no liability or settlement requirements exist.

Even though it is mandatory in any "sales transaction method" to guarantee that contractual promises will be kept, once agreed upon (first, by delivering the goods or services and second by paying for them), as noted by the Examiner in his reasoning for combining Fleming and Rosen, such reasoning does not apply to the trigger system, since it differs completely from such methods by dealing solely with storage and delivery of credentials.

The trigger system aims to allow impersonation of one's financial credentials by someone else other than the accountholder with complete anonymity by the one performing any subsequent sales transaction and making use of the previously stored authorization provided by a trigger server. It has as its main purpose, to facilitate the transport of an asset while avoiding any liability that could relate from such asset transfer.

Even though credentials stored and forwarded by a trigger server are meant to be used in other sales transactions, trigger transactions themselves (the act of storing and forwarding credentials) cannot be compared to sales transactions or sales transaction systems because they serve different purposes at different points in time, thus providing a support system over a disconnected model which maintains itself completely unrelated to any subsequent sales transactions which use of authorizations stored and provided by a trigger server.

A "trigger", which may also be called a "Programmable Impersonating Coupon for Store and Forward Devices", works like a digital "locker" purchased to store financial credentials and specific delivery conditions in any memory-capable device, from a computer to a cell phone (a trigger server), with the intent of later delivering such credentials to another device capable of then attempting a "sales transaction" based upon these credentials.

Such sales transaction attempts can occur either via the systems of Rosen or Fleming or via any other regular sales transaction method (like a regular ATM withdrawal, Credit Card, etc...).

Such ability to trigger other sales transactions to be attempted by devices capable of using credentials that are acquired, stored and delivered by a trigger server without participation in the transactions themselves is what contrasts the trigger method, according to the invention, from all other sales systems or methods currently described in the prior art.

The trigger system is not meant to perform any sales transaction nor to participate in any settlement related to such transactions. It has nothing to do with the delivery of services or merchandise or any transfer of funds or settlement. The trigger authorization collection and delivery system is completely unaware of any subsequent sales transaction that might occur using credentials supplied by a trigger server and it is not involved in any transaction-related issues since its only obligation is to collect, store and deliver someone's credential information to other systems which engage in the transactions themselves.

The reason for charging a fee for the trigger service is quite simple: People will pay to have their credentials collected, stored and disbursed to an impersonator, who intends to use such credentials on other systems on unrelated subsequent sales/payment transaction attempts. Such a charge for collecting and forwarding one's credentials can occur on a per transaction basis, or can be contractually licensed to the systems making use of the trigger authorization store and forward capabilities (either the same or another account or payment method can be used to pay for the storage and delivery of the credential being safeguarded and delivered by the trigger system).

To repeat, the comparison of the trigger system, according to the invention, to Fleming and Rosen fails because none of these prior art systems even resemble the functionality inherent in the trigger system. The trigger system does not perform any sales transaction; it is not involved with merchandise, services or payments; it does not participate in any settlement or settlement related issues; and, actually, it has as its basic principle to avoid engaging in any kind of sale and correlated liabilities by solely providing storage and delivery for one's authorization information necessary for other systems to perform transactions themselves.

The trigger method does not provide, as other methods do, a conduit for the exchange of goods or services against payments. It is a service (product) all in itself, purchased independently as a commitment from a trigger server to store and deliver authorization information to be used by other transactions on other systems based on a secret code given to the purchaser of such storage and programmable impersonation delivery rights.

In contrast to Rosen, a trigger transaction is not a sales transaction commitment whereby, once the transaction is agreed upon, none can interfere with the outcome of the transaction. It does allow full control for interfering with the conditions in which future sales transactions can occur by controlling the circumstances under which other systems can make use of such credentials. Subsequent transaction attempts making use of an authorization stored and forwarded by a trigger server can be used either in conjunction with

Fleming, Rosen or any other kind of "Sale against Payment" method, as long as such devices are capable of receiving the financial credentials electronically from a trigger server.

The trigger method is not a method for effectuating "sales transactions" and therefore cannot be compared to any other such methods. It does use common communication equipment, such as ATMs, point-of-sale devices and other equipment, as well as known secret code and public/private key encryption methods, but through a whole new service concept that can be described as a "Programmable Impersonating Coupon".

Such Coupons work as stand-alone password-encrypted data packets made out of other hosts' access codes, not meant to exchange any product or asset, but to provide financial credentials which other sales systems and methods can make use of. When one presents an electronic request and another commits to the delivery of such an asset, a sales transaction is consummated and has to be settled one way or another. This is the main aspect that the trigger system intends to avoid: providing credential information so that other systems can perform transactions themselves without the trigger system being engaged in such transactions or involved in any related settlement or liability derived from them.

When customers receive goods and merchants receive payment, at minimum, two liabilities exist. A sales transaction generates necessarily two accountancies, one for the entity supplying the goods and another for the entity providing the payment. It also generates the need for settlement linking the move of the asset by the money module and the delivery of the goods promised by the merchant.

The trigger system completely ignores such aspects of current money transfer and sales methods focusing on the control of the programmable structure that stores and forwards the access packet (credentials). It intends to facilitate asset allocation by allowing secure access to the credentials that supply the assets and not to assets themselves. Its sole purpose is to allow easier access to goods and services by one using someone else's credentials through Programmable Impersonation Coupons.

The trigger system according to the invention will never participate in any actual sales transaction and therefore cannot be compared to systems and methods which do just that.

It is at the sole discretion of the host to allow its credentials to be stored and forwarded via the trigger server: to decide upon what to allow, log and expose about the access contained in host's credentials, that are stored and forwarded by the trigger server.

Even though trigger access packets bear some similarities to Microsoft's "electronic coins" (both are encrypted data packets based upon secret codes), they greatly differ in their usage and the type of information which they carry. And since trigger packets do not carry any intrinsic worth, they do not have to be unique, and do not have to exist in a single place. In contrast to electronic coins, they can be distributed in unlimited quantities without any asset duplication or concern about their duplication.

A Programmable Impersonation Coupon can be worth a lot or nothing and the only one in control of it is the holder of the access key (the credential supplier): the provider of the authorization.

A trigger transaction is, in essence, not a sale or a financial transaction and does not carry with it any liability aside from safeguarding the credential and guaranteeing its delivery to the presenter of the correspondent secret code under the predetermined conditions. It uses well-known public/private key encryption methods to protect the packages, without carrying any liability over the asset that such access could disburse. In the end, the trigger system needs no knowledge about the content of the credentials it stores and forwards.

Impersonation Coupons grant access to assets provided by account owners using customizable control over access impersonation delivery through properties that can be configured and modified. They can be used by a variety of clients capable of storing and forwarding Coupons under the protocol.

For example, someone else's account could provide a person $20 at an ATM machine say twice a week, or a pizza over the phone from home only, say twice a month on weekends. One could provide a cap of $50 per month, or medicine, or groceries, or any other conceivable asset.

The system allows Coupons to be moved from machine to machine, storing and forwarding another host's access packets verifiable by a key signature given to the purchaser of the storage (service). Once the protocol is acknowledged between machines, several different applications can develop methods and properties to implement it, extending its capacity and configuration possibilities.

For example, a device capable of knowing the correct date and time can utilize a configurable parameter that accepts the expiration date on the Coupon. Another device capable of detecting the phone number from where you are calling, can allow, or not allow, access unless from an specific area or phone.

Claim 1 of this application recites a system, and claim 10 recites a method, which allows impersonation of someone else's account under controllable circumstances. Many other uses of such an Impersonating Coupon will become apparent to those skilled in the art; applicant's claims are not meant to exclude any of them just by not being capable of predefining each possible one.

Because the trigger system does not guarantee the availability of the asset it is intended to grant, its disposal and storage become less complicated and its importance in the overall process diminishes. The owner can always modify and cancel any Coupon by using the secret key for the Coupon.

Another facility when operating with Coupons is the ability to store them in multiple copies, something that no other asset-based contract can provide at the present time. Imagine the same money belonging to two different accounts, or two vehicle titles being issued for the same car. These are problems that do not exist with triggers since two different people can have access to the credential at the host's and owner's discretion over the type of access such authorization will provide.

When dealing with the Internet, Impersonation Coupons can easily be broadcast and stored among several different machines and devices and that alone makes them unlike any other form of asset transfer, because they do not transfer any asset. Due to the fact that the access can be revoked at any time by the controller of the secret code, they cannot be considered anything more than a formal intention to provide someone something: something someone would only possess (if ever) once a Coupon were accepted back and verified by the host controller of the account.

Because the package itself does not carry with it any worth, it can be duplicated and or destroyed, or coexist in many different places at the same time without duplicity or loss of liquidity.

The owner of an asset can provide others controlled access to it based upon programmable parameters that can be distributed to various machines, deemed to express the conditions and circumstances where such access to assets shall be granted.

In short, the trigger system is a unique form of asset transfer support system, which provides distributed transferability, full anonymity and no liability or settlement implications unlike any other system currently available.

Accordingly, applicant's independent claims 1 and 10, and therefore also dependent claims 2-9 and 11-18, distinguish patentably over both Fleming and Rosen, taken either individually or in combination. This application is therefore believed to be in condition for immediate allowance. A formal Notice of Allowance is respectfully solicited.

Respectfully submitted,

By
Karl F. Milde, Jr.
Reg. No. 24,822

MILDE & HOFFBERG, LLP
10 Bank Street - Suite 460
White Plains, NY 10606
(914) 949-3100

I hereby certify that this correspondence is being deposited with the United States Postal Services as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, DC 20231 on 5-24-02

MILDE & HOFFBERG, LLP

By

Date 5-24-02